Improving power grid cybersecurity



he Information Trust Institute (ITI) (iti.illinois.edu) at the University of Illinois Urbana-Champaign (UIUC) has a broad research portfolio in the field of information security and has been researching issues related to electric power infrastructure and the development of a stronger, more resilient grid. Their research efforts have significantly contributed to the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project. Ten years ago, the electricity sector was largely "security unaware." Since then, thanks in part to TCIPG, the industry has broadly adopted security best practices. That transition came about through breakthrough research, national expert panels, and the writing of key documents. Because the threat landscape continuously evolves, however, it is essential to maintain resiliency in a dynamic environment and ensure continuous improvement.

The TCIPG project (http://tcipgpro.cpanel. engr.illinois.edu), a partnership among Illinois and three other leading US universities— Dartmouth College, Arizona State University, and Washington State University—as well as governmental and industrial organizations, looks for ways to protect the grid's underlying computing and communication network infrastructure from malicious attacks as well as from accidental causes, such as natural disasters, misconfiguration, or operator errors. TCIPG participants continually collaborate with the national laboratories and the utility sector to improve the way that power grid infrastructure is designed.

TCIPG comprises several dozen researchers, students, and staff who bring interdisciplinary expertise essential to the operation and public adoption of current and future grid systems. That expertise extends to power engineering; computer science and engineering; advanced communications and networking; smartgrid markets and economics; and science, technology, engineering and mathematics (STEM) education.

TCIPG research in smart grid resiliency

Countering threats to the nation's cyber systems in critical infrastructure such as the power grid has become a major strategic objective and was identified as such in Homeland Security Presidential Directive 7 [1]. Smart-grid technologies promise advances in efficiency, reliability, integration of renewable energy sources, customer involvement, and new markets. But to achieve those benefits, the grid must rely on a cyber-measurement and control infrastructure that includes components ranging from smart appliances at customer premises to automated generation control. Control systems and administrative systems no longer have an air gap; security between the two has become more complicated and complex.

TCIPG research has produced important results and innovative technologies in addressing that need and the complexity by focusing on the following areas:

- Detecting and responding to cyberattacks and adverse events, as well as incident management of these events;
- ▶ Securing of the wide-area measurement system on which the smart grid relies;

- Maintaining power quality and integrating renewables at multiple scales in a dynamic environment; and
- Developing advanced test beds for experiments and simulation using actual power system hardware "in the loop."

Much of this work has been achieved because of the success of the experimental test bed.

Test bed cross-cutting research

Experimental validation is critical for emerging research and technologies. The TCIPG test bed enables researchers to conduct, validate, and evolve cyberphysical research from fundamentals to prototype, and finally, transition to practice. It provides a combination of emulation, simulation, and real hardware to realize a large-scale, virtual environment that is measurable, repeatable, flexible, and adaptable to emerging technology while maintaining integration with legacy equipment. Its capabilities span the entire power grid—transmission, distribution and metering, distributed generation, and home automation and control. Together, these provide true end-to-end capabilities for the smart grid.

The cyber-physical test bed facility uses a mixture of commercial power system equipment and software, hardware and software simulation, and emulation to create a realistic representation of the smart grid. This representation can be used to experiment with nextgeneration technologies that span communications from generation to consumption and everything in between. In addition to offering a realistic environment, the test bed facility has cutting-edge research and commercial instruments that can explore problems from multiple dimensions, tackling indepth security analysis and testing, visualization and data mining, and federated resources, and developing novel techniques that integrate these systems in a composable way. "Composable" means each part of the system is secure and continues to be secure when joined to all the other parts.

A parallel project funded by the state of Illinois, the Illinois Center for a Smarter Electric Grid (ICSEG), is a five-year project to develop and operate a facility to provide services for the validation of information

technology and control aspects of smart-grid systems, including microgrids and distributed energy resources. This project's key objective is to test and validate in a laboratory setting how new and more cost-effective smart-grid technologies, tools, techniques, and system configurations can be used in trustworthy configurations to significantly improve those in common practice today. The laboratory is also a resource for smart-grid equipment suppliers and integrators and electric utilities to allow validation of system designs before deployment.

Education and outreach

In addition to basic research, TCIPG has addressed needs in education and outreach. Nationally, there is a shortage of professionals who can fill positions in the power sector. Skills required for smart-grid engineers have changed dramatically. Graduates of the collaborating TCIPG universities are well-prepared to join the cyber-aware grid workforce as architects of the future grid, as practicing professionals, and as educators.

Continuing education

In the area of continuing education, TCIPG:

- Conducts short courses for practicing engineers and for Department of Energy (DOE) program managers;
- Holds a biennial TCIPG Summer School for university students and researchers, utility and industry representatives, and government and regulatory personnel;
- Organizes a monthly webinar series featuring thought leaders in cybersecurity and resiliency in the electricity sector; and
- ▶ Conducts extensive STEM outreach to K-12 students and teachers. (TCIPG has developed interactive, open-ended apps (iOS, Android, MinecraftEdu) for middle-school students, along with activity materials and teacher guides to facilitate integration of research, education, and knowledge transfer by linking researchers, educators, and students.)

The electricity industry in the United States is made up of thousands of utilities, equipment and software vendors, consultants, and regulatory bodies. In both its National Science Foundation (NSF)-funded and DOE/Department of Homeland Security (DHS)-funded phases, TCIPG has actively developed extensive relationships with such entities and with other researchers in the sector, including conducting joint research with several national laboratories.

The involvement of industry and other partners in TCIPG is vital to its success and is facilitated by an extensive Industry Interaction Board (IIB) and a smaller External Advisory Board (EAB). The EAB, with which they interact closely, includes representatives from the utility sector, system vendors, and regulatory bodies, in addition to the DOE Office of Electricity Delivery and Energy Reliability and the DHS Office of Science and Technology.

Partnerships and impact

While university led, TCIPG has always stressed real-world impact and industry partnerships. That is why TCIPG technologies have been adopted by the private sector.

- Several TCIPG technologies have been or are currently deployed on a pilot basis in real utility environments.
- A leading equipment vendor adopted their advanced technologies for securing embedded systems in grid controls.
- Three start-up companies in various stages of launch employ TCIPG foundational technologies.

To read more about TCIPG, visit http://tcipg.org.

[Photo credit: SeanPavonePhoto/iStock/Thinkstock]

